UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Dawn Appel, Jody Burgstahler, Kevin Burgstahler, Robert Etten, Jennifer Harris, and Glenn Jaspers, on behalf of themselves and all others similarly situated, Plaintiffs, v. Equifax, Inc., Defendant.	Case No: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Dawn Appel, Jody Burgstahler, Kevin Burgstahler, Robert Etten, Jennifer Harris, and Glenn Jaspers ("Plaintiffs"), by their undersigned counsel, for themselves and all others similarly situated, hereby commence this class action suit against Defendant Equifax, Inc. ("Equifax" or "Defendant"), and allege as follows:

NATURE OF ACTION

1. On September 7, 2017, Equifax publicly announced that hackers had compromised its servers and accessed the highly-sensitive personal and financial information of over 143 million U.S. consumers. From mid-May through July 2017, hackers had access to the names, addresses, social security numbers, and birth dates—among other items of personal information—of over half of the United States population with a credit history. This breach (the "Equifax Data Breach") was discovered on July 29, 2017.

2. Equifax, the oldest and one of the largest American credit reporting agencies, reports annual revenue of approximately $3.1 billion. Equifax "organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide." Its databases also include data on employees from over 7,100 employers.[1]

3. This action is brought on behalf of both a proposed Nationwide Class and Minnesota Subclass of individuals whose highly-sensitive personal identifying and financial information ("Personal Data") was made available to unauthorized third parties due to Equifax's negligent conduct.

4. Hackers exploited weak points in the software on Equifax's website to gain access to the data housed on Equifax's servers. The information contained on those servers was compromised for over two months before the breach was detected by Equifax.

5. Plaintiffs and the proposed class of consumers were harmed by Equifax's inadequate data security practices. Plaintiffs seek to represent themselves, a nationwide class of all consumers in the United States, and a Minnesota Subclass of all consumers in Minnesota whose Personal Data was compromised as a result of Equifax's actions.

6. Plaintiffs bring this lawsuit on behalf of all similarly situated consumers—individuals whose Personal Data was compromised as a result of Equifax's conduct—and

[1] Equifax, *Company Profile,* http://www.equifax.com/about-equifax/company-profile/ (last accessed Sept. 12, 2017).

allege that Equifax's conduct violates the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.*, and was tortious under common law principles.

7. Plaintiffs also bring this lawsuit on behalf of consumers residing in Minnesota whose Personal Data was compromised as a result of Equifax's conduct. Plaintiffs allege that Equifax's conduct violates Minnesota's Data Breach Notification Statute, Minn. Stat. § 325E.61.

8. On behalf of themselves and the Classes, Plaintiffs seek actual damages, statutory damages, punitive damages, and equitable and declaratory relief.

PARTIES

9. Plaintiff Dawn Appel is an individual who resides in Maple Grove, Minnesota and was a citizen of the State of Minnesota during the period of the Equifax Data Breach.

10. Plaintiff Jody Burgstahler is an individual who resides in Hastings, Minnesota and was a citizen of the State of Minnesota during the period of the Equifax Data Breach.

11. Plaintiff Kevin Burgstahler is an individual who resides in Hastings, Minnesota and was a citizen of the State of Minnesota during the period of the Equifax Data Breach.

12. Plaintiff Robert Etten is an individual who resides in Roseville, Minnesota and was a citizen of the State of Minnesota during the period of the Equifax Data Breach.

13. Plaintiff Jennifer Harris is an individual who resides in Brooklyn Park, Minnesota and was a citizen of the State of Minnesota during the period of the Equifax Data Breach.

14. Plaintiff Glenn Jaspers is an individual who resides in Savage, Minnesota and was a citizen of the State of Minnesota during the period of the Equifax Data Breach.

15. Defendant Equifax, Inc., is a Georgia corporation with its headquarters and principal place of business located in Atlanta, Georgia. Defendant operates through its various subsidiaries that include Equifax Information Services, LLC, and Equifax Consumer Services, LLC (also known as Equifax Personal Solutions or "PSOL").

FACTUAL ALLEGATIONS

16. On September 7, 2017, Equifax announced that its servers had been hacked and that the Personal Data of nearly 143 million Americans had been compromised.

17. The Equifax Data Breach occurred from mid-May to July 2017. Equifax detected the breach on July 29, 2017, and five weeks later, on September 7, publicly confirmed that approximately 143 million consumers' Personal Data had been compromised.

18. The Personal Data compromised included an expansive range of information, including names, addresses, social security numbers, dates of birth, identification numbers (e.g., driver's license, military ID, or passport), credit card numbers, and records of credit disputes.

19. The security breach of the highly-sensitive personal identifying and financial information stored on Equifax's servers has created a substantially increased risk of identity theft to the Class for the foreseeable future.

20. The risks to consumers created by disclosure of the Personal Data may continue indefinitely. A person's name and social security number are unlikely to change, as that process is long, complex, and carries with it associated difficulties and costs.

21. The Personal Data made available as a result of the Equifax Data Breach is a goldmine for criminals who wish to engage in identity theft or other fraud. For example, a social security number is used to identify individuals and authenticate their identity, both by the government and private companies. The value of social security numbers to criminals exponentially increases when stolen with other personal information, such as name, address, and birth date—the kinds of data also compromised in the Equifax Data Breach.

22. Each type of Personal Data stolen in the breach has independent financial value in the black market. A social security number sells for $3, and other information commands a price as well; e.g., a mother's maiden name sells for $6. These various pieces of personal information become more valuable when provided together.

23. Identity theft occurs when a criminal uses a person's personal identifying information, such as the Personal Data released in the Equifax Data Breach, to commit fraud or other crimes. The kinds of personal identifying information that can be used for identity theft include a person's name, email address, mailing address, social security number, billing and shipping addresses, and telephone number.

24. According to a 2012 report published by the Federal Trade Commission, the "range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions," and "any privacy framework should recognize additional harms that might arise from unanticipated uses of data." There is "significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."

25. Because Plaintiffs' and Class members' social security numbers were disclosed without authorization for an improper purpose, they face an imminent, immediate, and continuing increased risk of identity theft and identity fraud. This risk will only increase over time, and the value on the black market of their social security numbers will continue to rise.

26. According to a 2017 report by Javelin Strategy & Research, individuals whose personal identifying information is subject to a reported security breach (such as the Equifax Data Breach) are more likely than the general public to suffer identity theft or identity fraud. In 2016, the total amount stolen through identity theft reached approximately $16 billion.

27. According to the FTC, victims of identity theft and identity fraud are at serious risk of substantial losses. Once identity thieves have a consumer's personal information, the thieves can then drain the person's bank account, run up charges on their credit cards, open new accounts, get medical treatment on their health insurance, or fraudulently file tax returns and collect tax refunds.

28. When identity thieves open financial accounts and incur charges in a victim's name, it can be especially damaging. It may take some time for the victim to become aware of the theft, even as it causes significant harm to the victim's credit rating and finances.

29. Compared to other pieces of personal identifying information, social security numbers are incredibly difficult to change, and the risk of their misuse can continue indefinitely into the future. In order to obtain a new social security number, a person must provide evidence that someone is using the number fraudulently, as well as demonstrate that he or she has done all he can to fix the problems resulting from the misuse. In other words, a person whose social security number has been stolen cannot obtain a new social security number until the damage has already been done.

30. Obtaining a new social security number only reduces the likelihood of continued identity fraud; it does not absolutely prevent it. The effects of the identity theft may persist long after the incident because government agencies, private businesses, and credit reporting agencies likely still have the person's records under the old number. In fact, a new social security number may create additional problems for a person's credit history. When positive credit information is not associated with the new social security number, it can more difficult to obtain credit or obtain favorable credit terms due to the absence of a credit history.

Equifax's Inadequate Security Practices

31. Equifax's security practices with regards to Class Members' Personal Data were negligent. Equifax did not follow best practices or take adequate care to protect consumers' Personal Data.

32. Storing social security numbers and other Personal Data in a central location increases their usefulness for data analysis, but it raises the risk that hackers can take them all at once, as occurred here with the Class Members' Personal Data.

33. The Equifax Data Breach is not the first time in recent years—or even in recent months—that hackers have gained access to sensitive data maintained by Equifax. In 2016, identity thieves stole critical W-2 tax and salary data from an Equifax-controlled website. Earlier in 2017, hackers were once again able to steal W-2 tax data from another Equifax subsidiary, TALX. These earlier breaches put Equifax on notice of the heightened and immediate risks of its inadequate security practices.

34. Furthermore, the particular vulnerability exploited by hackers in the Equifax Data Breach was known to Equifax months before the breach occurred. Months before the July 2017 breach, the Apache Software Foundation alerted Equifax to a vulnerability in its web-application software Apache Struts. This vulnerability was the one ultimately exploited by hackers that led to the Equifax Data Breach. In March 2017, the Apache Software Foundation provided clear and simple instructions on how to remedy the vulnerability—instructions Equifax simply ignored and failed to follow.

35. The Equifax Data Breach was not inevitable; it was a result of Equifax's neglect and underinvestment in the development of adequate security measures. There is

no technical reason that Equifax could not have directed its considerable resources to strengthening its security before the Equifax Data Breach. There is no reason that Equifax could have not implemented a software patch that would have eliminated the vulnerability and greatly reduced the risk to consumers. Instead, Equifax chose not to, instead waiting until 143 million individuals suffered harm.

Equifax's Ineffective Post-Breach Remedies

36. Equifax has failed to offer effective remedies to Class members following the announcement that millions of individuals' Personal Data was compromised.

37. On a website designed to address consumers' concerns and questions following the Equifax Data Breach, Equifax provides a link to sign up for its "TrustedID Premier" credit monitoring service.

38. Equifax currently offers a single year of free credit monitoring through the "TrustedID" service. The free sign-up offer will end on November 21, 2017. Beyond this free year, consumers must pay additional fees if they wish to continue credit monitoring through the service.

39. The risk of misuse of Plaintiffs' and Class members' compromised Personal Data will not end after a year. This risk will not disappear after two, or even five years. The risk to Plaintiffs and Class members will continue indefinitely.

40. The "TrustedID" service provided by Equifax only provides a monitoring service for consumers' credit activity, and does not provide services to remediate any harms arising from unauthorized use of the Personal Data exposed in the Equifax Data Breach.

41. Meaningful and effective identity theft monitoring and identity theft insurance are widely recognized as necessary tools for every person whose personal identifying information is taken. After the June 2015 data breach at the U.S. Office of Personnel Management, the federal government provided identity theft monitoring, identity theft insurance, and restoration services to all 21.5 million victims affected by the breach. In other words, the United States recognized that victims of this kind of data breach need these type of services when their sensitive Personal Data is exposed.

42. Plaintiffs and Class members may also find it necessary to place "credit freezes" on their accounts with Equifax and the other credit reporting agencies in order to protect themselves from future identity theft. A credit freeze operates by restricting access to an individual's credit report and preventing new lines of credit from being taken out—unless the individual provides a secure PIN to "thaw" the credit report. There are attendant costs to both "freezing" and "thawing" the reports imposed by the credit agencies, and the process must be done separately with each credit reporting agency in order to be fully effective.

43. The wide-ranging inadequacies of Equifax's security practices are evident even in their response to the breach. Consumers seeking to freeze their Equifax credit reports were given PINs directly based upon the date and time that the freeze was set up, rather than the PINs being randomly assigned. Although this practice for assigning PINs was changed after public outcry, it demonstrates Equifax's lack of attention to security measures even in the wake of what has been deemed the most serious data breach in American history.

44. After facing a similar backlash about its continued practice of charging for freezing credit reports, Equifax announced that it will provide free credit freezes for thirty days, beginning September 12, 2017. However, after this period, Equifax will continue to charge for credit freezes and thaws, and will potentially make a profit as consumers act to protect themselves from the fallout of the Equifax Data Breach.

JURISDICTION AND VENUE

45. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A). There is minimal diversity and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

46. Additionally and alternatively, this Court has original jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiffs bring claims arising under federal law based on Equifax's violations of the FCRA, 15 U.S.C. § 1681 *et seq.* The Court has supplemental jurisdiction over the remaining claims pursuant to 28 U.S.C. § 1367(a).

47. Venue is proper in the District of Minnesota because Equifax regularly transacts business in this District, a substantial part of the events or omissions giving rise to the claims occurred in this District, and the Plaintiffs and some of the Class Members reside in this District.

CLASS ACTION ALLEGATIONS

48. Plaintiffs incorporate the allegations in each above numbered paragraph.

49. Plaintiffs bring this action on behalf of themselves and all others similarly situated.

50. Plaintiffs seek to represent the following Classes, defined *infra*:

Nationwide Class

> All persons residing in the United States or its territories whose Personal Data was accessed by unauthorized individuals in the Equifax Data Breach announced by Equifax on September 7, 2017.

Minnesota Subclass

> All persons residing in Minnesota whose Personal Data was accessed by unauthorized individuals in the Equifax Data Breach announced by Equifax on September 7, 2017.

51. The Classes are so numerous that individual joinder of all its members is impracticable. While the precise number and identification of Class members is unknown to Plaintiffs at this time and can be ascertained only through appropriate discovery of Defendant, the Nationwide Class is believed to number approximately 143 million. The Minnesota Subclass is believed to number over 2 million.

52. This action is brought and may properly be maintained as a class action pursuant to the provisions of Federal Rules of Civil Procedure 23(a)(1)-(4) and 23(b)(1)-(3). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions. Common questions of fact and law exist as to all Class members which predominate over any questions affecting only individual Class members. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any Class member, include the following:

a. Whether Equifax failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the Class members' Personal Data;

b. Whether Equifax failed to ensure adequate protection against known and anticipated threats to security;

c. Whether Equifax owed a duty to protect Plaintiffs' and the Class members' Personal Data;

d. Whether Equifax followed best practices concerning its IT security;

e. Whether Equifax's conduct was intentional, willful, or negligent;

f. Whether Equifax violated the FCRA;

g. Whether Equifax was negligent;

h. Whether Equifax was unjustly enriched;

i. Whether Equifax violated Minnesota's data breach notification laws;

j. Whether Plaintiffs and the Class members suffered damages; and

k. Whether Plaintiffs and the Class members are entitled to injunctive, declaratory, and monetary relief as a result of Equifax's conduct.

53. Plaintiffs' claims are typical of the claims of the Class members. Plaintiffs and other Class members must prove the same facts in order to establish the same claims, described herein, which apply to all Class members.

54. Plaintiffs are adequate representatives of the Classes because they are members of the Class and their interests do not conflict with the interests of the Classes members they seek to represent. Plaintiffs have retained counsel competent and

experienced in the prosecution of complex class action, data breach, and consumer privacy litigation, and together Plaintiffs and their counsel intend to prosecute this action vigorously for the benefit of the Classes. The interests of Class members will be fairly and adequately protected by Plaintiffs and their counsel.

55. A class action is superior to other available methods for the fair and efficient adjudication of this litigation since individual litigation of the claims of all Class members is impracticable. Even if every Class member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts, in which individual litigation of thousands of cases (or more) would proceed. Individual litigation presents a potential for inconsistent or contradictory judgments, the prospect of a race for the courthouse, and an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation increases the expense and delay to all parties and the court system in resolving the legal and factual issues common to all Class members' claims relating to the Equifax Data Breach. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

56. The various claims asserted in this action are additionally or alternatively certifiable under the provisions of Federal Rules of Civil Procedure 23(b)(1) and/or 23(b)(2) because:

a. The prosecution of separate actions by millions of individual Class members would create a risk of inconsistent or varying adjudications with

respect to individual Class members, thus establishing incompatible standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class members would also create the risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of the other Class members who are not a party to such adjudications and would substantially impair or impede the ability of such non-party Class members to protect their interests; and

c. Defendant has acted or refused to act on grounds generally applicable to the entirety of each of the Classes, thereby making appropriate final declaratory and injunctive relief with respect to the Classes as a whole.

COUNT I
Negligence
(On Behalf of the Nationwide Class)

57. Plaintiffs incorporate the allegations in each above numbered paragraph.

58. Equifax owed a duty to Plaintiffs and the Nationwide Class to exercise reasonable care in obtaining, retaining, and safeguarding their Personal Data.

59. Equifax's duty to Plaintiffs and the Class included designing, maintaining, monitoring, and testing its security systems and procedures to ensure that Plaintiffs' and Class members' Personal Data was adequately secured.

60. Equifax owed a duty to Plaintiffs and the Class to implement intrusion detection processes that would detect a data breach in a timely manner.

61. Equifax had a duty to delete any Personal Data that was no longer needed to serve client needs and which it was not required to maintain by law.

62. Equifax's privacy policy acknowledges its duty to adequately protect Plaintiffs' and Class members' Personal Data, and identifies safeguarding privacy and security of personal information as a "top priority."

63. Equifax owed a duty to safeguard Plaintiffs' and Class members' Personal Data as set forth in the FCRA and under common law principles.

64. Equifax breached its duty by failing to maintain adequate data security practices, failing to detect the Equifax Data Breach in a timely manner, and failing to disclose that its data security practices were inadequate to safeguard the Personal Data.

65. Equifax knew or should have known that its failure to maintain adequate data security practices and technological safeguards would put Plaintiffs' and Class members' Personal Data at a high risk for unauthorized access.

66. But for Equifax's breach of its duties, Plaintiffs' and the Class members' Personal Data would not have been accessed by unauthorized individuals.

67. Plaintiffs and the Class members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

68. Equifax's breach of its duties is the proximate cause of the damages suffered by Plaintiffs and the Class members.

69. Plaintiffs seek actual damages and declaratory and injunctive relief on behalf of themselves and the Class.

COUNT II
Violation of the FCRA (15 U.S.C. § 1681 *et seq.*)
(On Behalf of the Nationwide Class)

70. Plaintiffs incorporate the allegations in each above numbered paragraph.

71. Equifax is a "consumer reporting agency" under the FCRA. 15 U.S.C. § 1681a(f).

72. The Personal Data released in the Equifax Data Breach is a "consumer report" under the FCRA. 15 U.S.C. § 1681a(d)(1).

73. Equifax was required to "maintain reasonable procedures" to prevent the release of consumer reports except as authorized by 15 U.S.C. § 1681b. 15 U.S.C. § 1681e(a).

74. None of the authorized purposes under § 1681b include the release of a consumer report to an unauthorized individual, such as a computer hacker.

75. Equifax willfully and/or recklessly failed to maintain reasonable procedures designed to limit the release of consumer reports as required by § 1681e(a). Equifax's willful and/or reckless conduct is supported by Equifax's previous data breaches, combined with the fact that Equifax's core business model involves data compilation and analysis of the wide array of information contained in consumer reports. Equifax was well aware of the importance of best data security practices and the associated risks of any data security failures.

76. Equifax's willful and/or reckless conduct provided the means for unauthorized hackers to obtain Plaintiffs' and Class members' Personal Data and consumer reports for no purpose deemed permissible under the FCRA.

77. Additionally and alternatively, Equifax's negligent conduct provided the means for unauthorized hackers to obtain Plaintiffs' and Class members' Personal Data and consumer reports for no purpose deemed permissible under the FCRA.

78. On behalf of themselves and the Class, Plaintiffs seek actual damages, statutory damages, punitive damages, and reasonable attorneys' fees and costs. 15 U.S.C. §§ 1681n(a), 1681o(a).

COUNT III
Unjust Enrichment
(On Behalf of the Nationwide Class)

79. Plaintiffs incorporate the allegations in each above numbered paragraph.

80. Equifax benefited from its unlawful acts through the receipt of payment in exchange for running credit checks and furnishing credit reports of Plaintiffs and the Class members. It would be inequitable to permit Equifax to retain the benefit of those payments, when its wrongful conduct in regard to those services injured Plaintiffs and the Class.

81. Plaintiffs and Class members have no adequate remedy at law for Equifax's wrongful conduct.

82. Plaintiffs seek restitution and equitable disgorgement to Plaintiffs and the Class members.

COUNT IV
Declaratory and Injunctive Relief
(On Behalf of the Nationwide Class)

83. Plaintiffs incorporate the allegations in each above numbered Paragraph.

84. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, the Court is authorized to enter a judgment declaring the parties' rights and legal relations, and grant further necessary relief based upon such a judgment.

85. Plaintiffs seek a judgment declaring, without limitation, that Equifax owed a legal duty to protect Plaintiffs' and Class members' Personal Data, that Equifax breached this duty, and that Equifax's breach caused the Equifax Data Breach and the resulting injuries to Plaintiffs and the Class.

86. Plaintiffs and the Class members face a threat of great and irreparable harm if, after a trial on the merits, a permanent injunction is not granted, in that Plaintiffs and the Class members face ongoing injury because of the Equifax Data Breach and the release of their Personal Data.

87. Plaintiffs and Class members have no adequate legal remedy to protect their interests from the ongoing harm described herein.

88. Plaintiffs seek injunctive relief including, without limitation, an order compelling Equifax to notify each Class member of the Equifax Data Breach, to provide complimentary credit monitoring and insurance to each Class member for a period of time to be determined by the Court in excess of the single year currently offered by Equifax, to provide credit freezes and thaws to each Class member indefinitely without charge, to establish a fund to which Class members may apply for reimbursement of the time and out-of-pocket expenses they incurred to prevent and/or remediate identity theft or identity fraud, and to discontinue its inadequate data security practices.

COUNT V
Violation of Minn. Stat. § 325E.61
(On Behalf of the Minnesota Subclass)

89. Plaintiffs incorporate the allegations in each above numbered Paragraph.

90. Under Minnesota Statute § 325E.61, subd. 1, any business that conducts business in Minnesota, and that owns or licenses data that includes personal information, is required to disclose any security breach of its system following the discovery that any resident of Minnesota whose unencrypted personal information was, or is reasonably believed, to have been acquired by an unauthorized person.

91. Businesses that maintain personal information that the business does not own are required to notify the owners of the information of any breach in the security of the data immediately following discovery if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

92. The Personal Data exposed in the Equifax Data Breach constitutes "personal information" as set out in Minn. Stat. § 325E.61, subd. 1(e).

93. Equifax violated the provision of § 325E.61 that mandates immediate notification of a breach by waiting over five weeks following the discovery of the breach before it notified the public at large.

94. Minn. Stat. § 325E.61, subd. 2 also requires that upon discovery of circumstances requiring notification to more than 500 persons, the person or business discovering the breach shall notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

95. Equifax failed to provide notification of its security breach to the other consumer reporting agencies within the required 48-hour time frame set out in Minn. Stat. § 325E.61, subd. 2.

96. Members of the Minnesota Subclass were injured by Equifax's unreasonable and inexcusable delay in providing notification of the Equifax Data Breach to both the owners of the Personal Data and to the other consumer reporting agencies.

97. Per Minn. Stat. § 8.31, any person injured by a violation of § 325E.61 may bring a civil action to recover damages, together with costs and disbursements, including costs of investigation and reasonable attorney's fees, and receive other equitable relief as determined by the court.

98. On behalf of themselves and the Minnesota Subclass, Plaintiffs seek actual damages, statutory damages, reasonable attorneys' fees and costs, and other equitable relief as determined by this court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment against Defendant as follows:

1. An Order certifying the Class and any appropriate subclasses thereof under the appropriate provisions of Federal Rule of Civil Procedure 23, and appointing Plaintiffs and their counsel to represent the Class;

2. Declarations that the actions of Defendant, as set out above, are unlawful;

3. Appropriate injunctive and equitable relief;

4. Compensatory damages;

5. Punitive damages;

6. Statutory damages;

7. Restitution and/or disgorgement;

8. Costs, disbursements, expenses, and attorneys' fees;

9. Pre- and post-judgment interest, to the extent allowable; and

10. Such other and further relief as this Court deems just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a trial by jury in this case as to all issues so triable.

Dated: September 29, 2017

Respectfully submitted,

s/ Daniel C. Hedlund

Daniel E. Gustafson (#202241)
Daniel C. Hedlund (#258337)
Joseph C. Bourne (#0389922)
Eric S. Taubel (#392491)
Kaitlyn L. Dennis (#0397433)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Telephone: (612) 333-8844
Facsimile: (612) 339-6622
Email: dgustafson@gustafsongluek.com
dhedlund@gustafsongluek.com
jbourne@gustafsongluek.com
etaubel@gustafsongluek.com
kdennis@gustafsongluek.com

ATTORNEYS FOR PLAINTIFFS AND THE PROPOSED CLASS